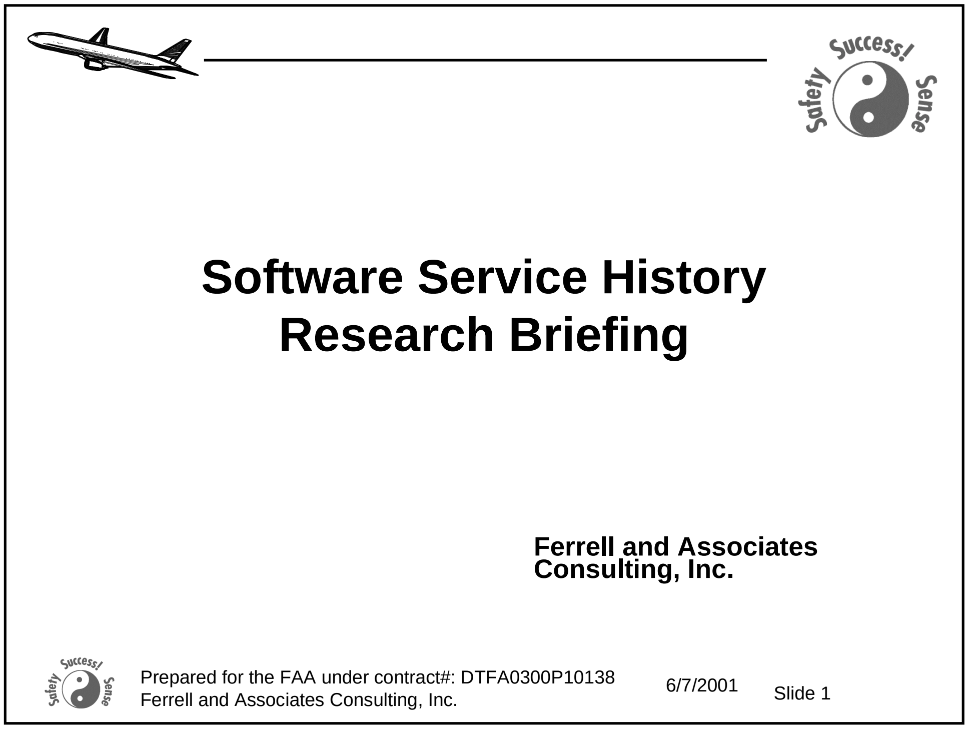
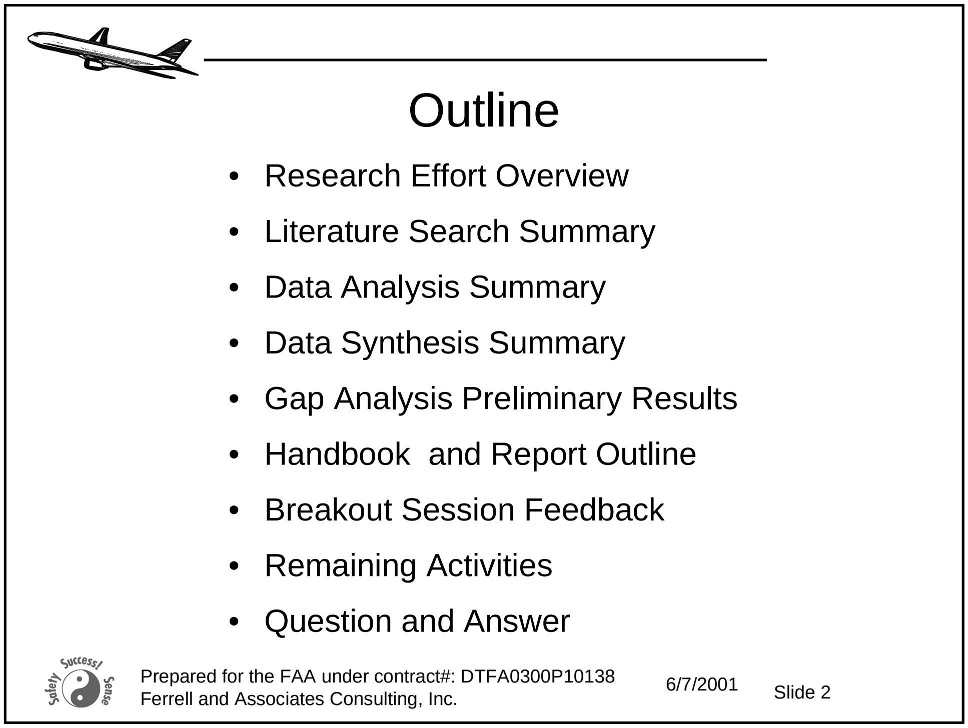


Software Service History
Research Briefing

Ferrell and Associates
Consulting, Inc.

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001 Slide 1

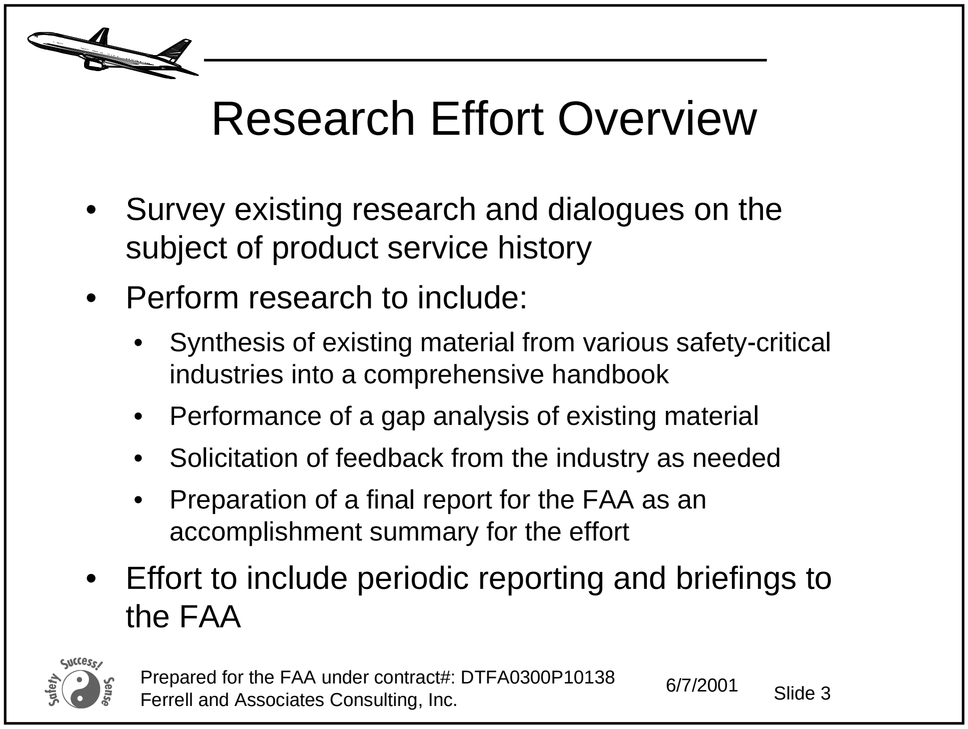


Outline

- Research Effort Overview
- Literature Search Summary
- Data Analysis Summary
- Data Synthesis Summary
- Gap Analysis Preliminary Results
- Handbook and Report Outline
- Breakout Session Feedback
- Remaining Activities
- Question and Answer

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

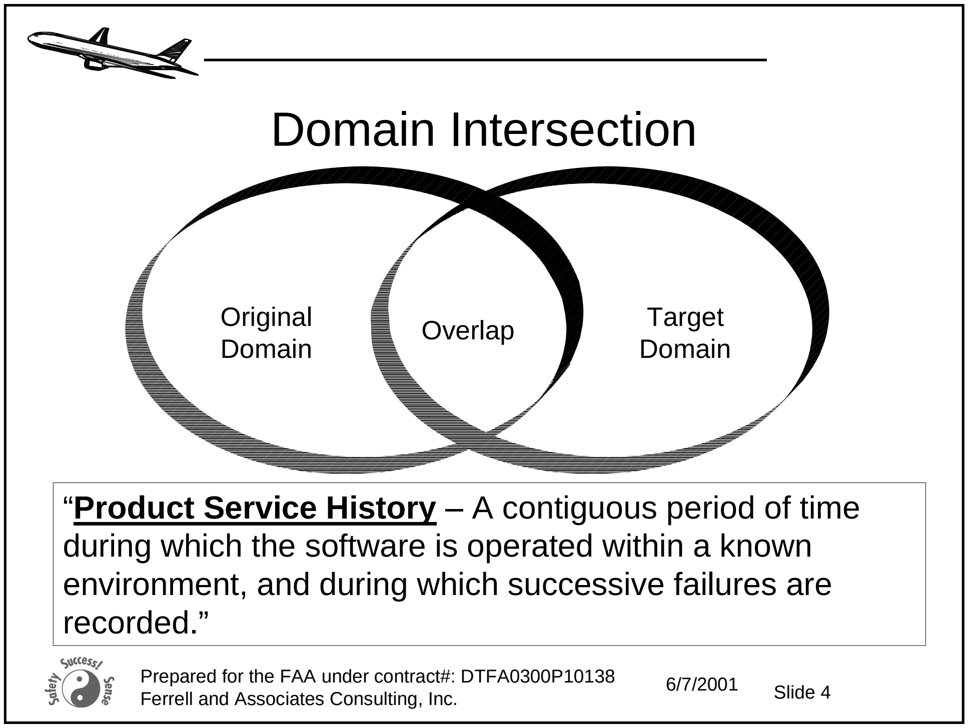
6/7/2001 Slide 2



Research Effort Overview

- Survey existing research and dialogues on the subject of product service history
- Perform research to include:
  - Synthesis of existing material from various safety-critical industries into a comprehensive handbook
  - Performance of a gap analysis of existing material
  - Solicitation of feedback from the industry as needed
  - Preparation of a final report for the FAA as an accomplishment summary for the effort
- Effort to include periodic reporting and briefings to the FAA

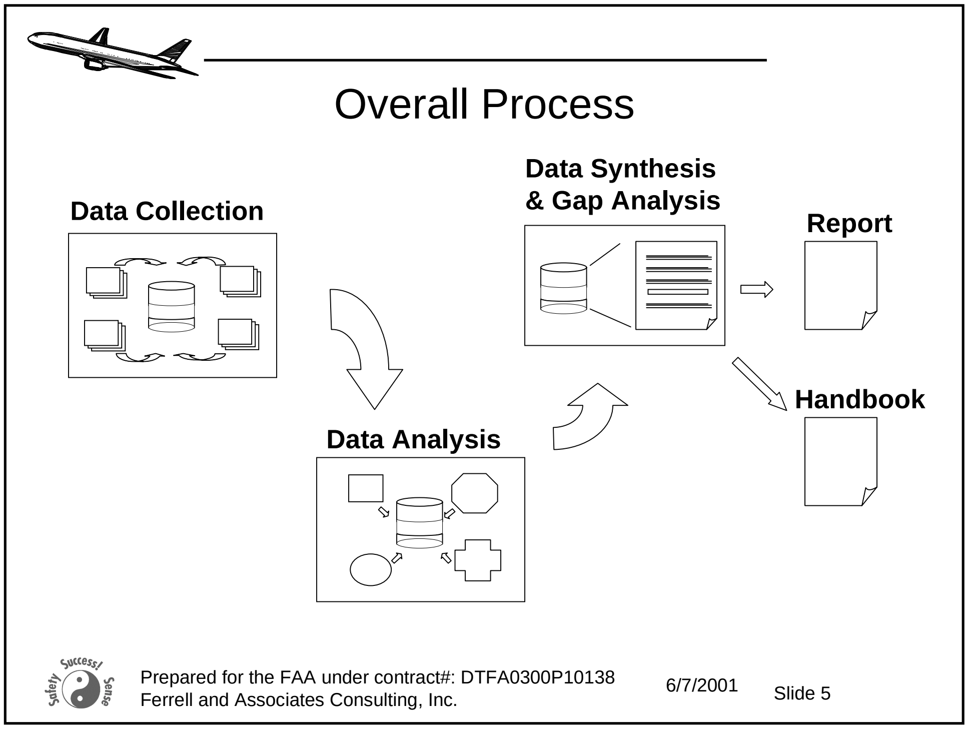
Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.
6/7/2001 Slide 3



Domain Intersection

"**Product Service History** – A contiguous period of time during which the software is operated within a known environment, and during which successive failures are recorded."

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.
6/7/2001 Slide 4



Overall Process

Data Collection

Data Analysis

Data Synthesis & Gap Analysis

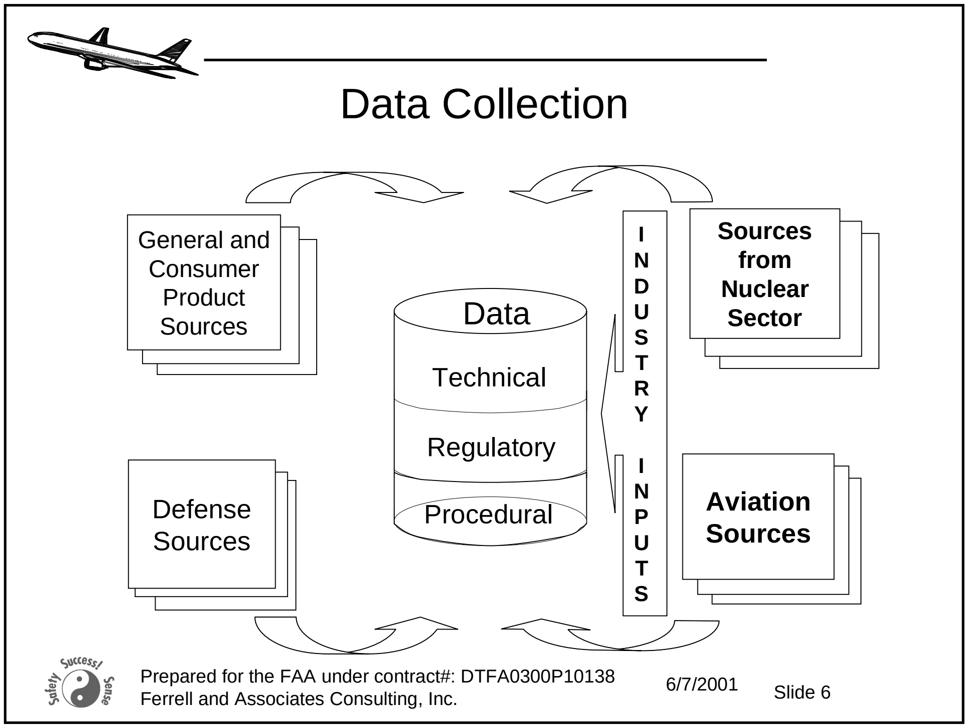
Report

Handbook

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

Slide 5



Data Collection

General and Consumer Product Sources

Defense Sources

Data

Technical

Regulatory

Procedural

INDUSTRY INPUTS

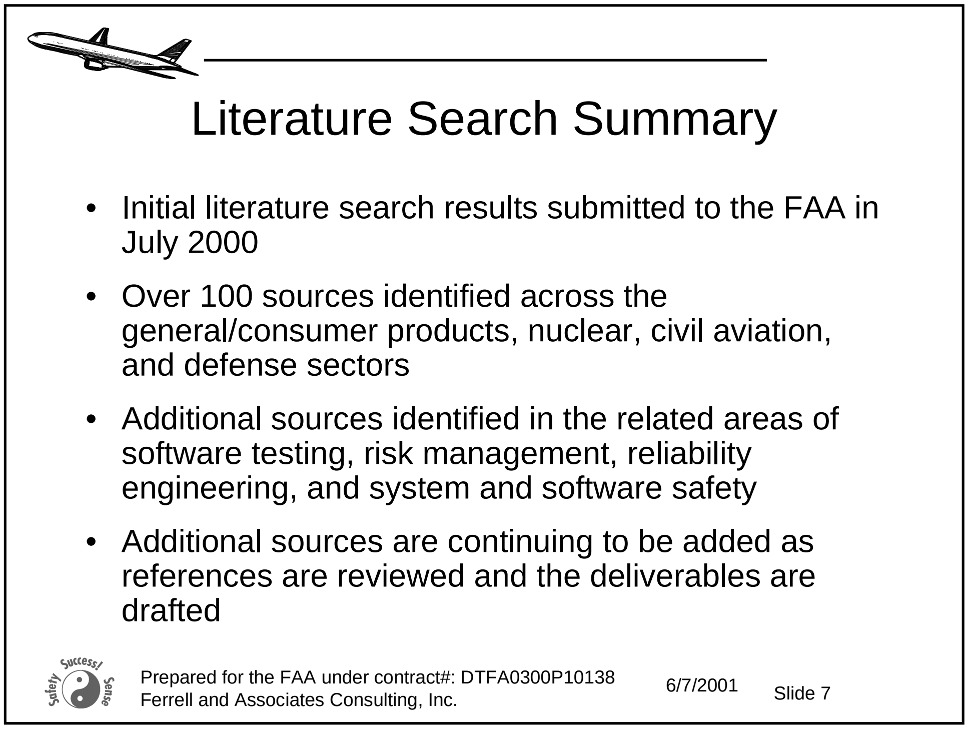
Sources from Nuclear Sector

Aviation Sources

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

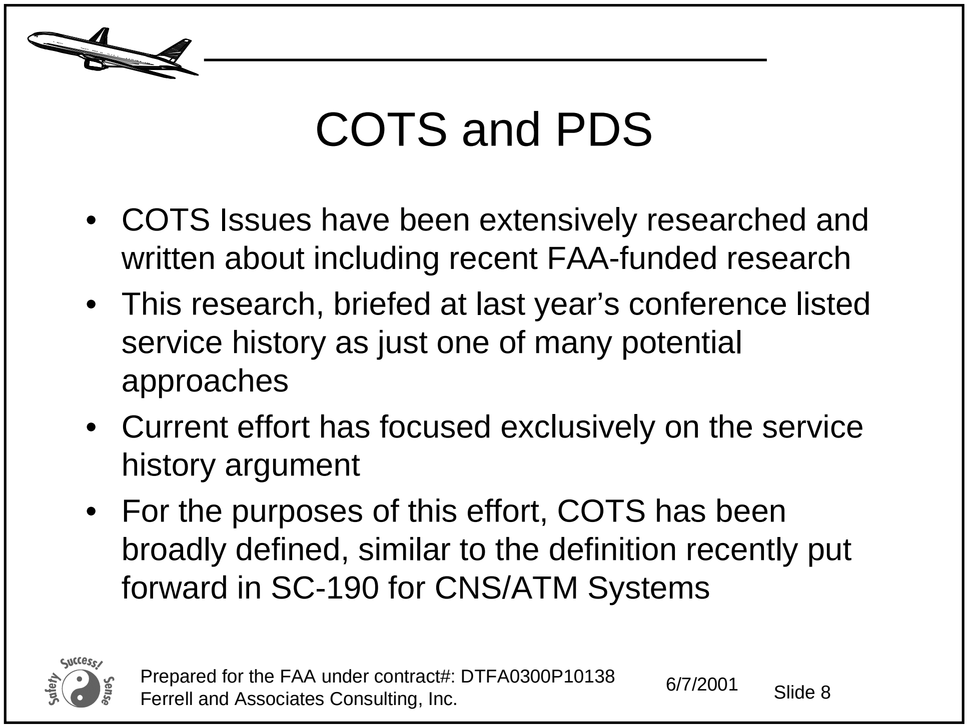
Slide 6



Literature Search Summary

- Initial literature search results submitted to the FAA in July 2000
- Over 100 sources identified across the general/consumer products, nuclear, civil aviation, and defense sectors
- Additional sources identified in the related areas of software testing, risk management, reliability engineering, and system and software safety
- Additional sources are continuing to be added as references are reviewed and the deliverables are drafted

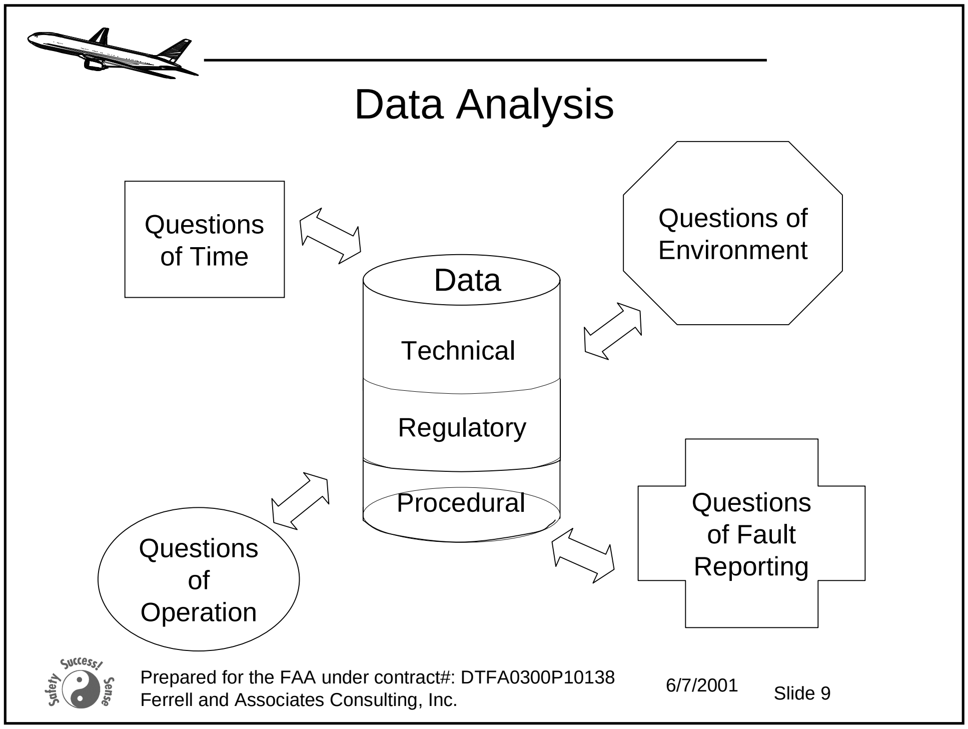
Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.
6/7/2001
Slide 7



COTS and PDS

- COTS Issues have been extensively researched and written about including recent FAA-funded research
- This research, briefed at last year’s conference listed service history as just one of many potential approaches
- Current effort has focused exclusively on the service history argument
- For the purposes of this effort, COTS has been broadly defined, similar to the definition recently put forward in SC-190 for CNS/ATM Systems

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.
6/7/2001
Slide 8



Data Analysis

Questions of Time

Questions of Environment

Data

Technical

Regulatory

Procedural

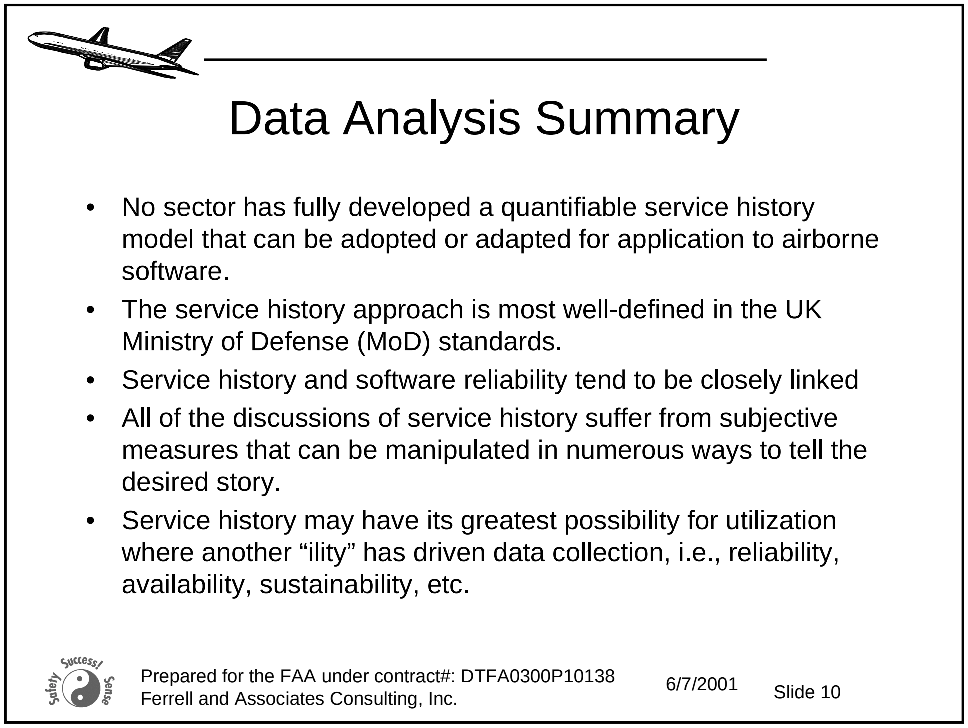
Questions of Operation

Questions of Fault Reporting

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

Slide 9



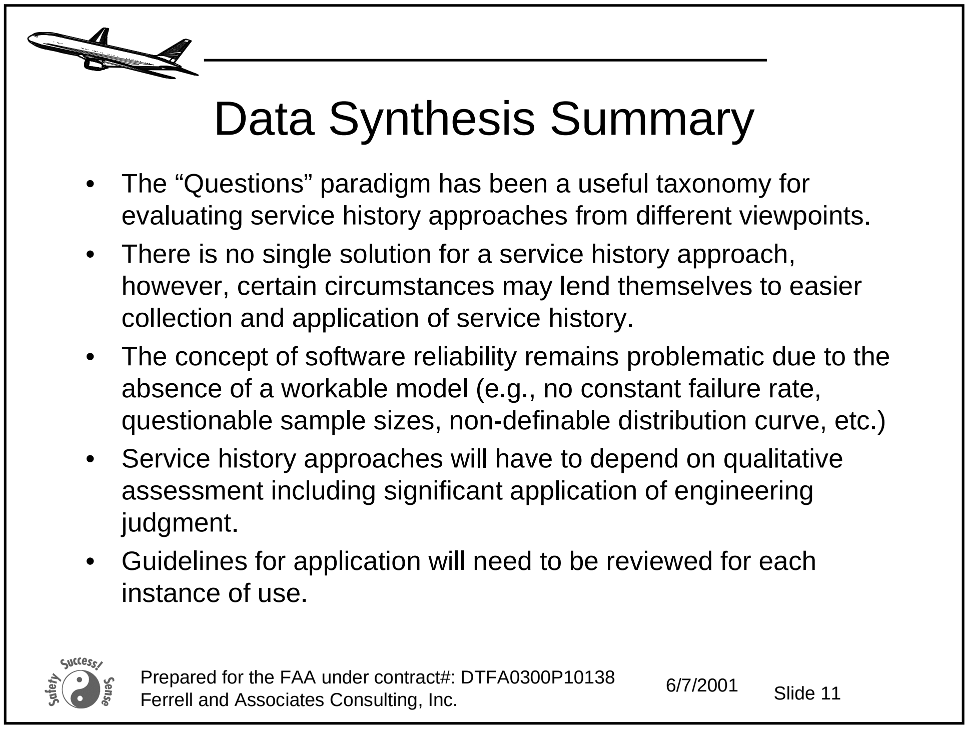
Data Analysis Summary

- No sector has fully developed a quantifiable service history model that can be adopted or adapted for application to airborne software.
- The service history approach is most well-defined in the UK Ministry of Defense (MoD) standards.
- Service history and software reliability tend to be closely linked
- All of the discussions of service history suffer from subjective measures that can be manipulated in numerous ways to tell the desired story.
- Service history may have its greatest possibility for utilization where another “ility” has driven data collection, i.e., reliability, availability, sustainability, etc.

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

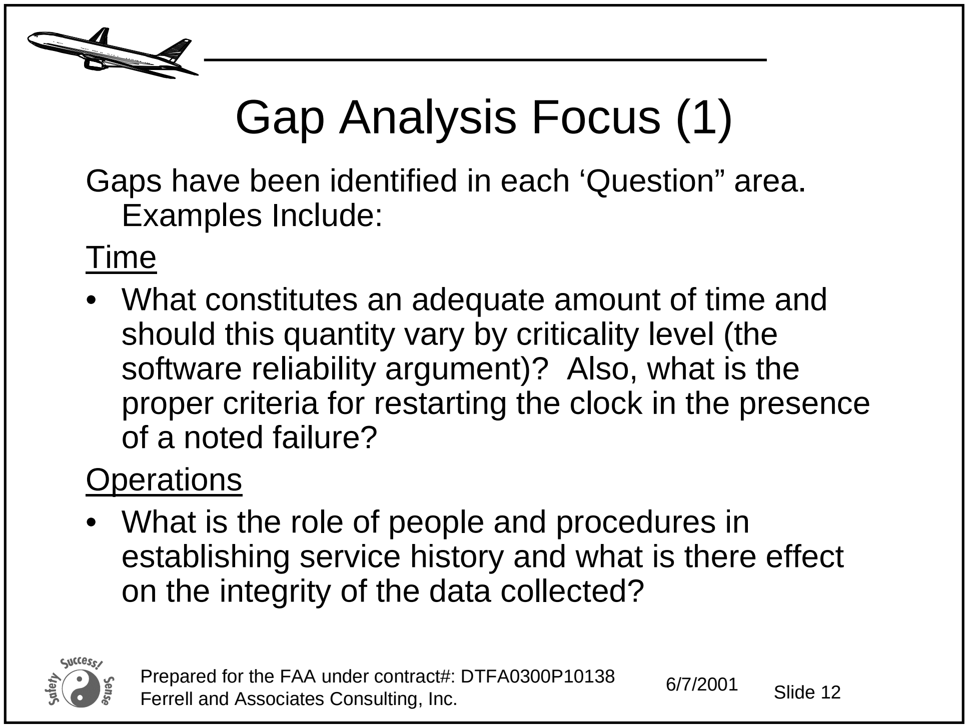
Slide 10



Data Synthesis Summary

- The “Questions” paradigm has been a useful taxonomy for evaluating service history approaches from different viewpoints.
- There is no single solution for a service history approach, however, certain circumstances may lend themselves to easier collection and application of service history.
- The concept of software reliability remains problematic due to the absence of a workable model (e.g., no constant failure rate, questionable sample sizes, non-definable distribution curve, etc.)
- Service history approaches will have to depend on qualitative assessment including significant application of engineering judgment.
- Guidelines for application will need to be reviewed for each instance of use.

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.
6/7/2001
Slide 11



Gap Analysis Focus (1)

Gaps have been identified in each ‘Question” area. Examples Include:

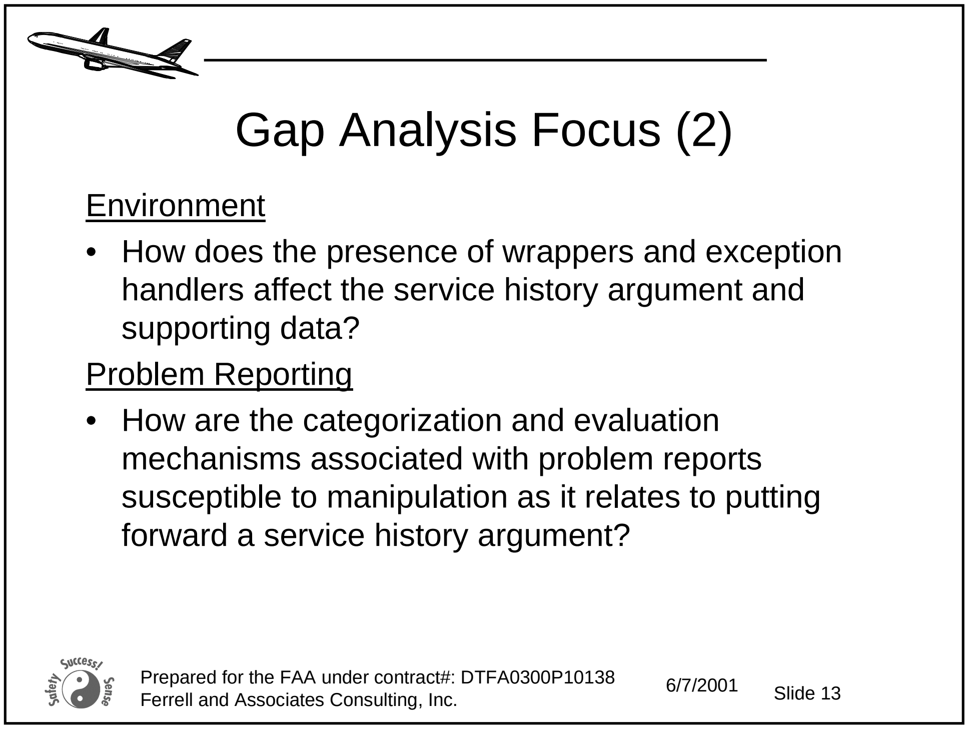
Time

- What constitutes an adequate amount of time and should this quantity vary by criticality level (the software reliability argument)? Also, what is the proper criteria for restarting the clock in the presence of a noted failure?

Operations

- What is the role of people and procedures in establishing service history and what is there effect on the integrity of the data collected?

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.
6/7/2001
Slide 12



Gap Analysis Focus (2)

Environment

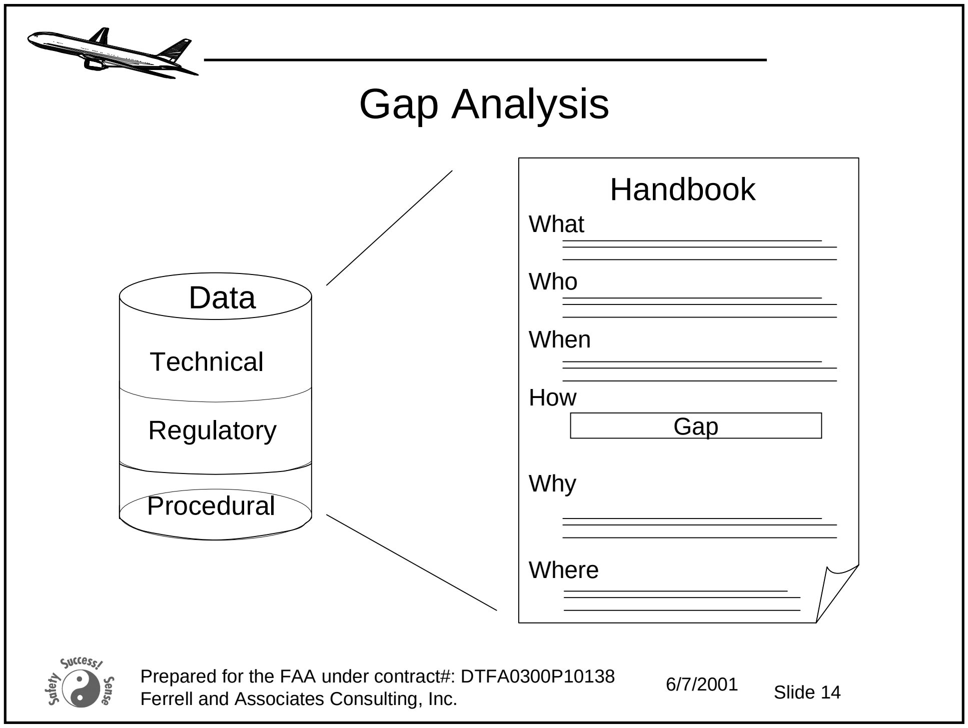
- How does the presence of wrappers and exception handlers affect the service history argument and supporting data?

Problem Reporting

- How are the categorization and evaluation mechanisms associated with problem reports susceptible to manipulation as it relates to putting forward a service history argument?

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001 Slide 13



Gap Analysis

Data

Technical

Regulatory

Procedural

Handbook

What

Who

When

How

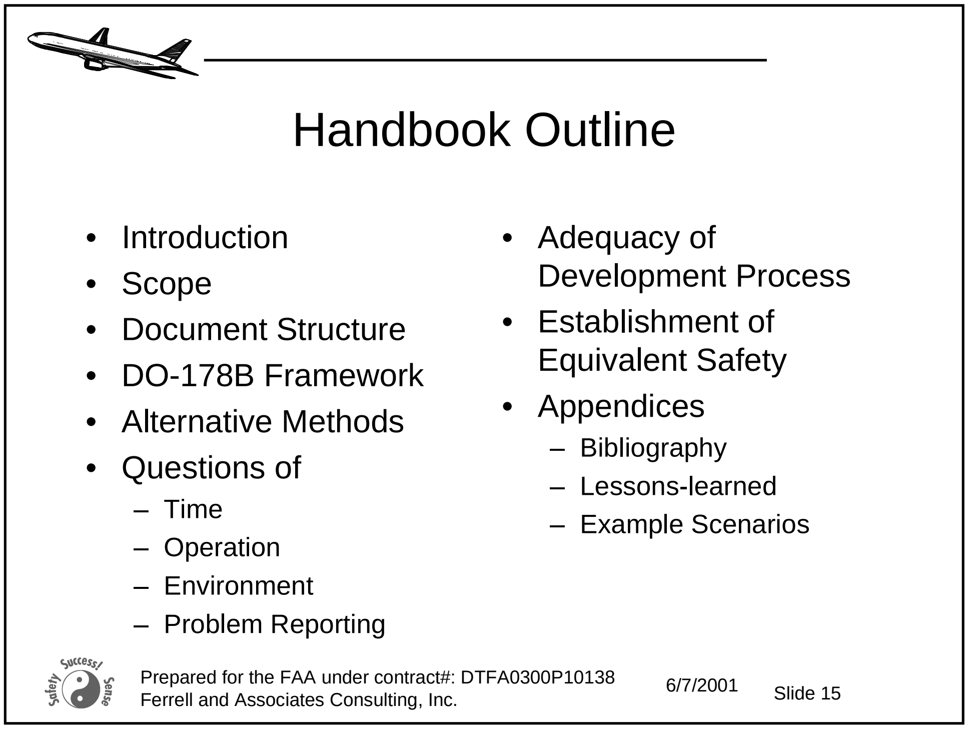
Gap

Why

Where

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001 Slide 14

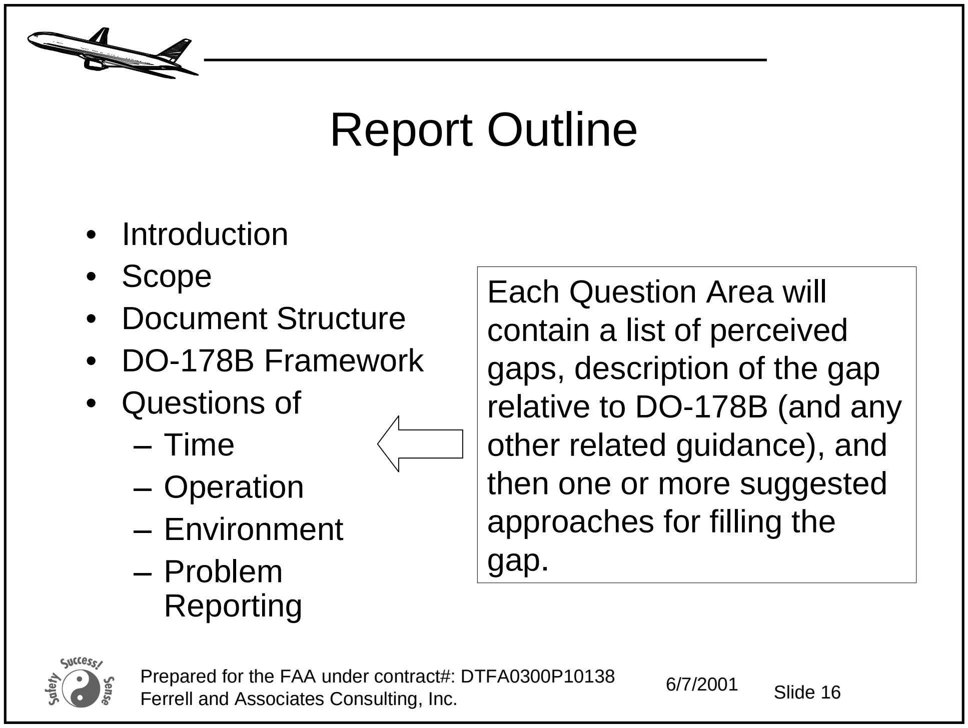


Handbook Outline

- Introduction
- Scope
- Document Structure
- DO-178B Framework
- Alternative Methods
- Questions of
  - Time
  - Operation
  - Environment
  - Problem Reporting
- Adequacy of Development Process
- Establishment of Equivalent Safety
- Appendices
  - Bibliography
  - Lessons-learned
  - Example Scenarios

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001 Slide 15



Report Outline

- Introduction
- Scope
- Document Structure
- DO-178B Framework
- Questions of
  - Time
  - Operation
  - Environment
  - Problem Reporting

Each Question Area will contain a list of perceived gaps, description of the gap relative to DO-178B (and any other related guidance), and then one or more suggested approaches for filling the gap.

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

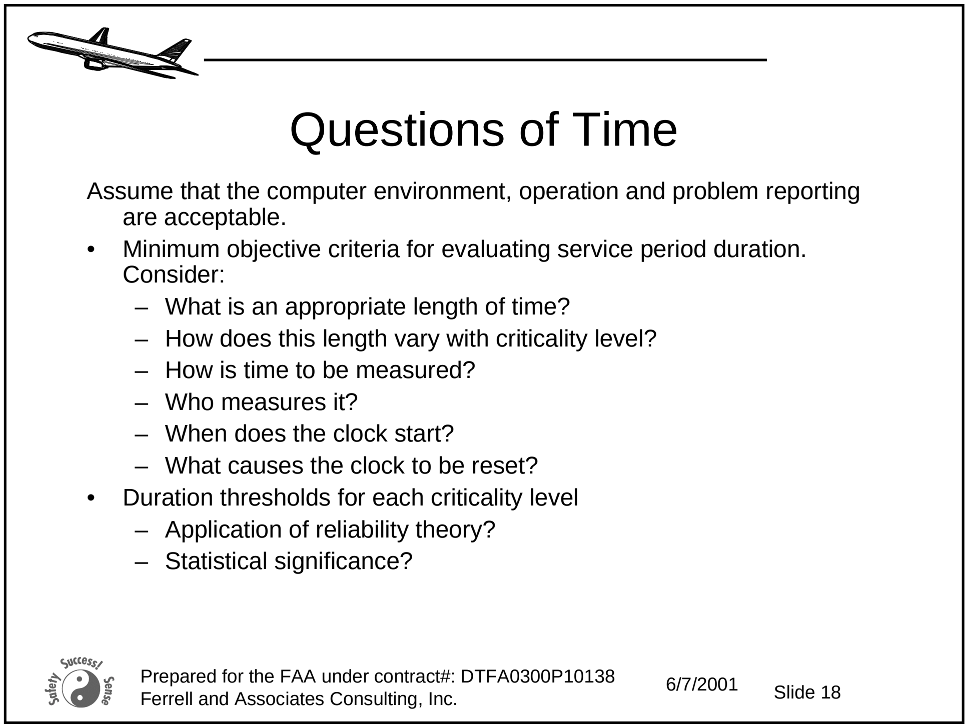
6/7/2001 Slide 16

Breakout Session Feedback

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

Slide 17



Questions of Time

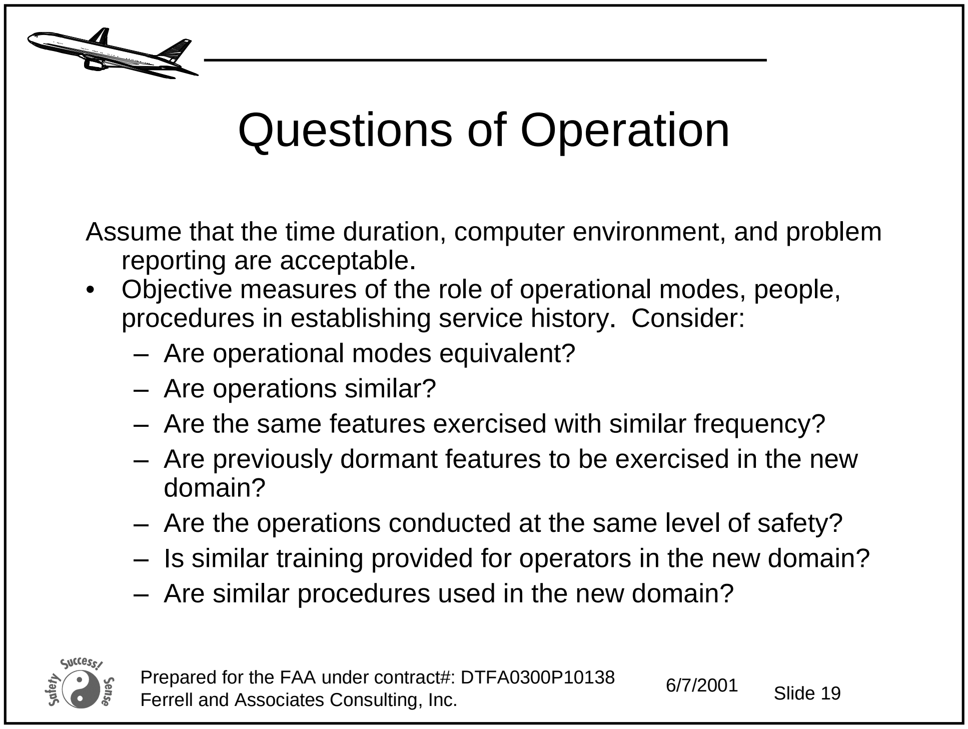
Assume that the computer environment, operation and problem reporting are acceptable.

- Minimum objective criteria for evaluating service period duration. Consider:
  - What is an appropriate length of time?
  - How does this length vary with criticality level?
  - How is time to be measured?
  - Who measures it?
  - When does the clock start?
  - What causes the clock to be reset?
- Duration thresholds for each criticality level
  - Application of reliability theory?
  - Statistical significance?

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

Slide 18



Questions of Operation

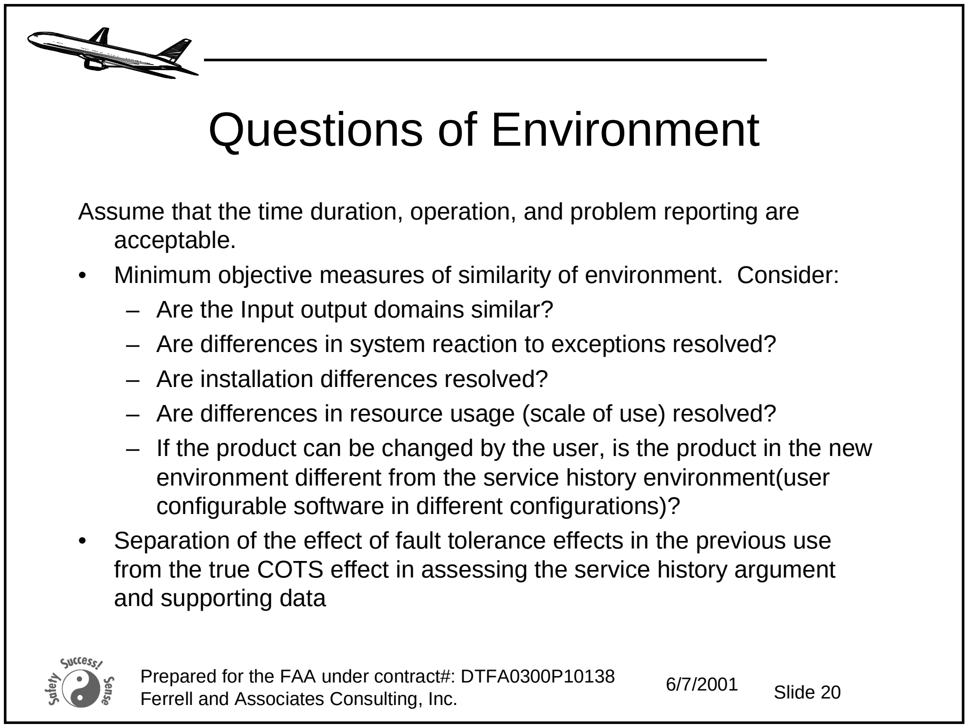
Assume that the time duration, computer environment, and problem reporting are acceptable.

- Objective measures of the role of operational modes, people, procedures in establishing service history. Consider:
  - Are operational modes equivalent?
  - Are operations similar?
  - Are the same features exercised with similar frequency?
  - Are previously dormant features to be exercised in the new domain?
  - Are the operations conducted at the same level of safety?
  - Is similar training provided for operators in the new domain?
  - Are similar procedures used in the new domain?

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

Slide 19



Questions of Environment

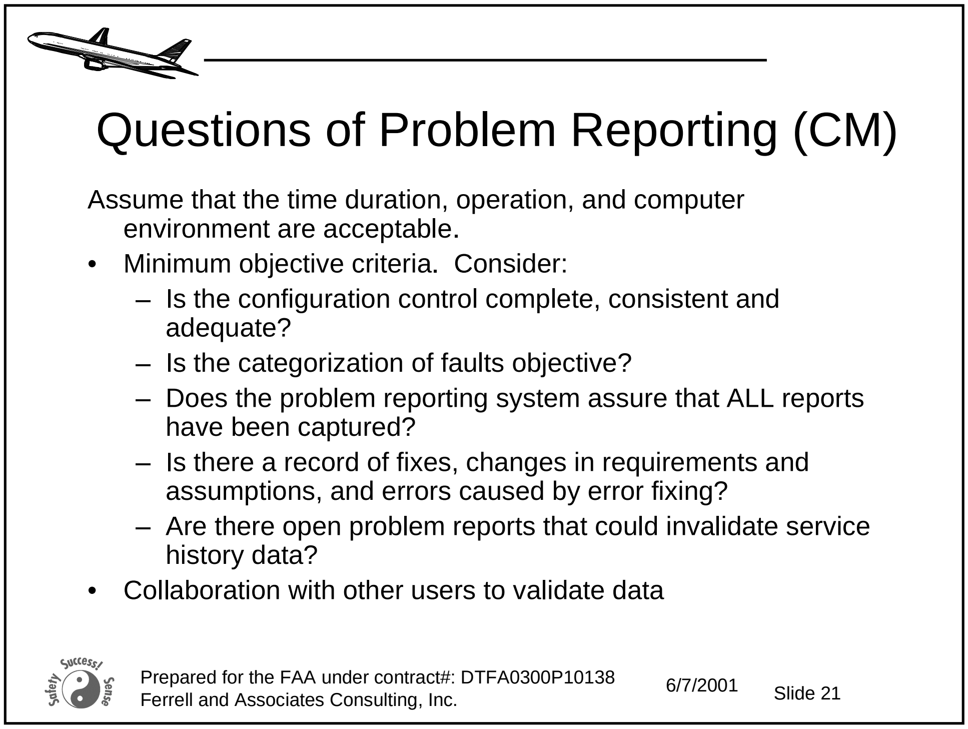
Assume that the time duration, operation, and problem reporting are acceptable.

- Minimum objective measures of similarity of environment. Consider:
  - Are the Input output domains similar?
  - Are differences in system reaction to exceptions resolved?
  - Are installation differences resolved?
  - Are differences in resource usage (scale of use) resolved?
  - If the product can be changed by the user, is the product in the new environment different from the service history environment(user configurable software in different configurations)?
- Separation of the effect of fault tolerance effects in the previous use from the true COTS effect in assessing the service history argument and supporting data

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

Slide 20



Questions of Problem Reporting (CM)

Assume that the time duration, operation, and computer environment are acceptable.

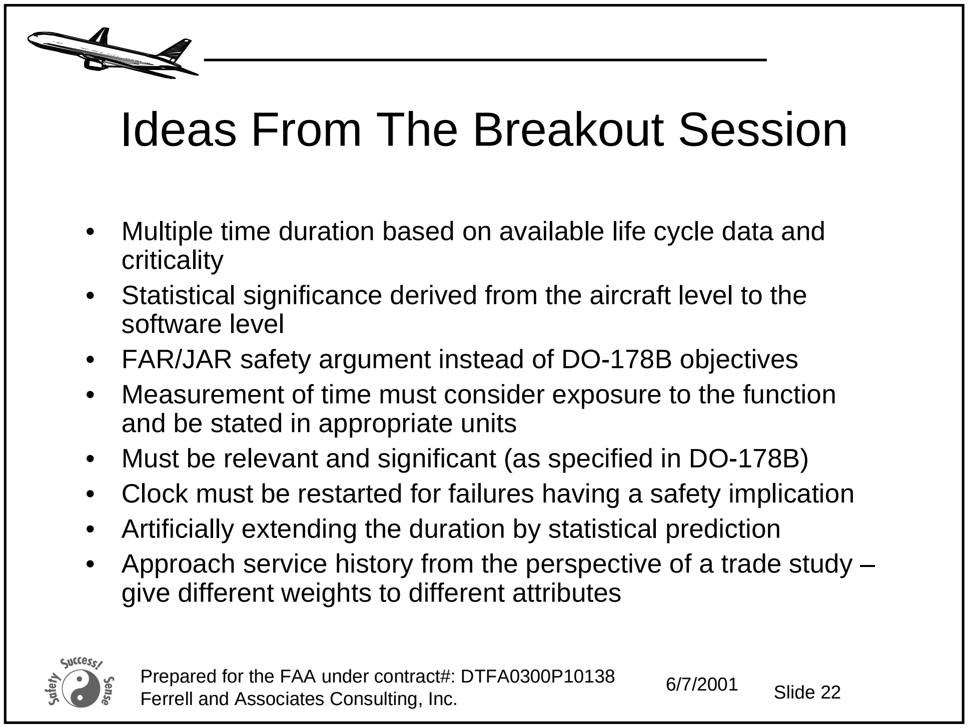
- Minimum objective criteria. Consider:
  - Is the configuration control complete, consistent and adequate?
  - Is the categorization of faults objective?
  - Does the problem reporting system assure that ALL reports have been captured?
  - Is there a record of fixes, changes in requirements and assumptions, and errors caused by error fixing?
  - Are there open problem reports that could invalidate service history data?
- Collaboration with other users to validate data

Safety Success! Sense

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

Slide 21



Ideas From The Breakout Session

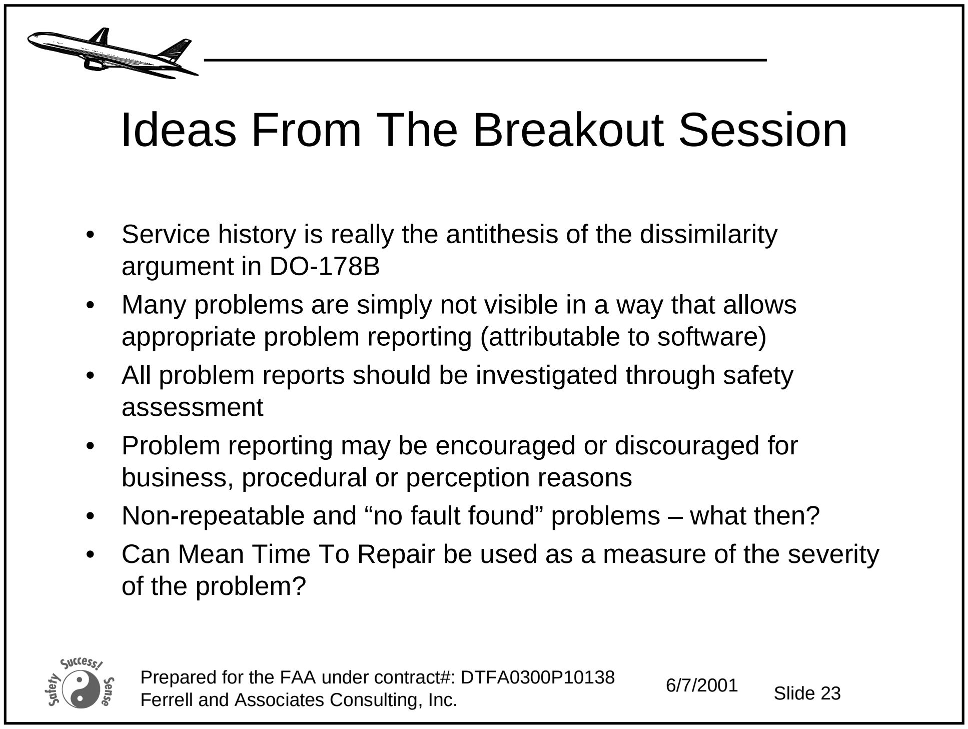
- Multiple time duration based on available life cycle data and criticality
- Statistical significance derived from the aircraft level to the software level
- FAR/JAR safety argument instead of DO-178B objectives
- Measurement of time must consider exposure to the function and be stated in appropriate units
- Must be relevant and significant (as specified in DO-178B)
- Clock must be restarted for failures having a safety implication
- Artificially extending the duration by statistical prediction
- Approach service history from the perspective of a trade study – give different weights to different attributes

Safety Success! Sense

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

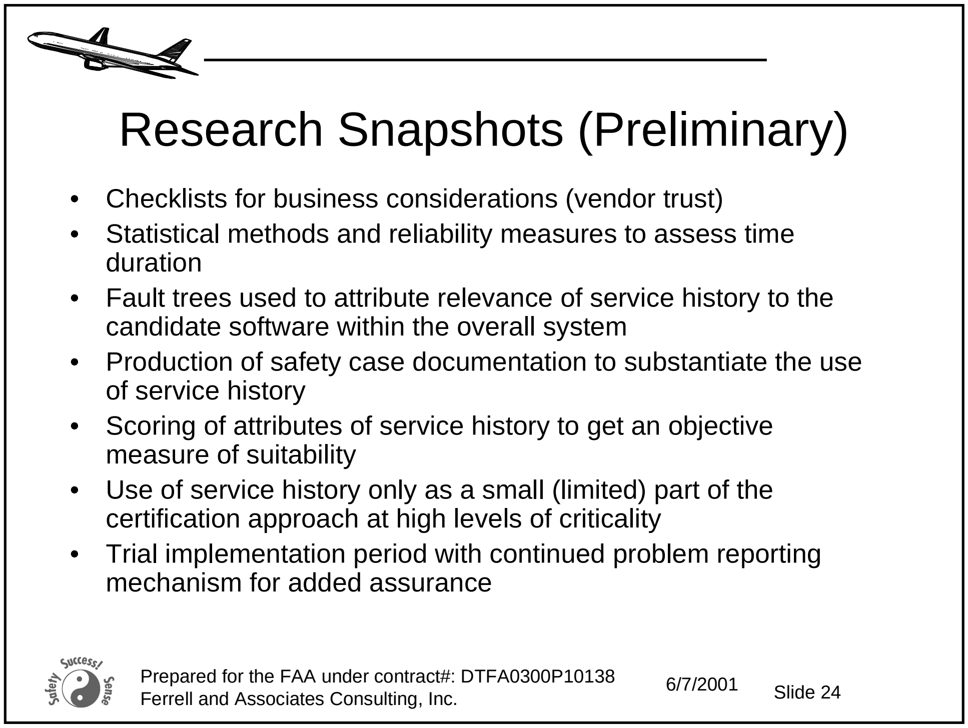
Slide 22



Ideas From The Breakout Session

- Service history is really the antithesis of the dissimilarity argument in DO-178B
- Many problems are simply not visible in a way that allows appropriate problem reporting (attributable to software)
- All problem reports should be investigated through safety assessment
- Problem reporting may be encouraged or discouraged for business, procedural or perception reasons
- Non-repeatable and “no fault found” problems – what then?
- Can Mean Time To Repair be used as a measure of the severity of the problem?

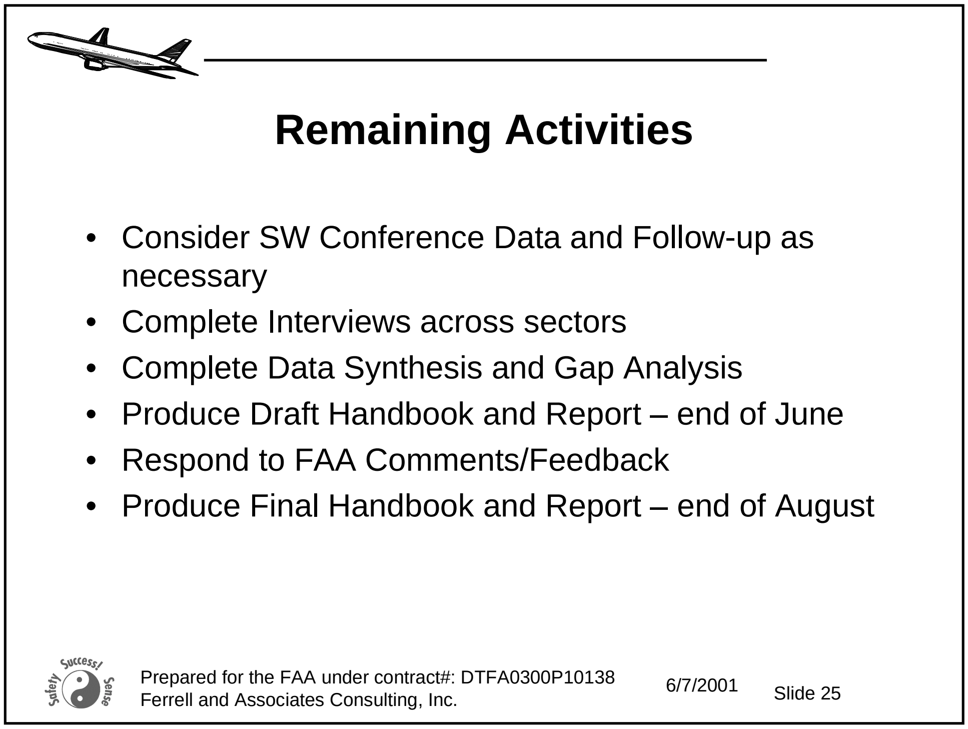
Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc. 6/7/2001 Slide 23



Research Snapshots (Preliminary)

- Checklists for business considerations (vendor trust)
- Statistical methods and reliability measures to assess time duration
- Fault trees used to attribute relevance of service history to the candidate software within the overall system
- Production of safety case documentation to substantiate the use of service history
- Scoring of attributes of service history to get an objective measure of suitability
- Use of service history only as a small (limited) part of the certification approach at high levels of criticality
- Trial implementation period with continued problem reporting mechanism for added assurance

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc. 6/7/2001 Slide 24



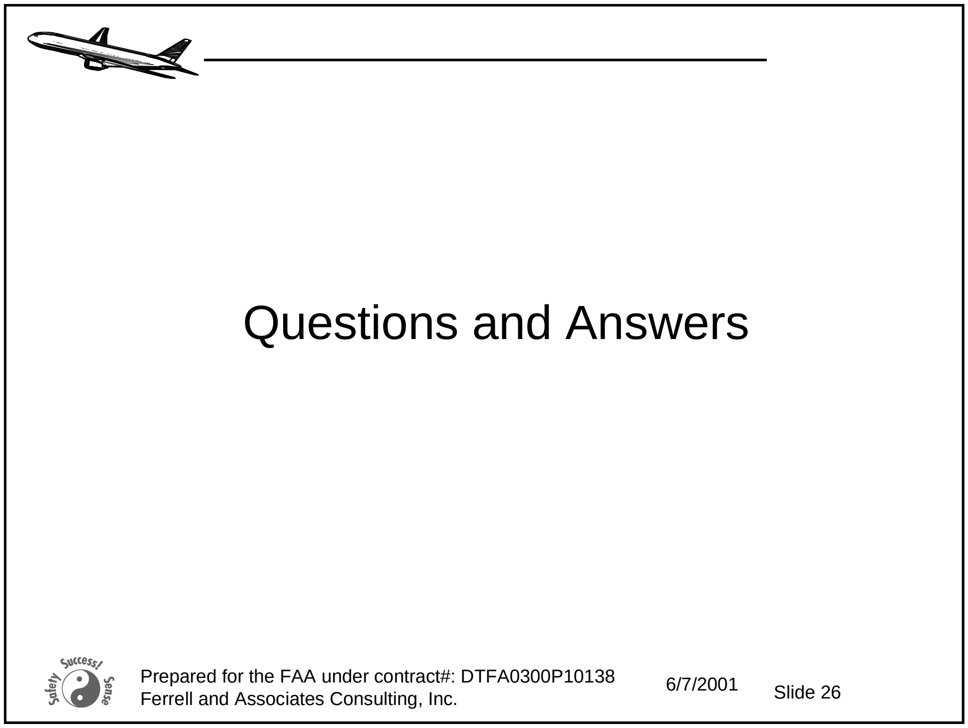
Remaining Activities

- Consider SW Conference Data and Follow-up as necessary
- Complete Interviews across sectors
- Complete Data Synthesis and Gap Analysis
- Produce Draft Handbook and Report – end of June
- Respond to FAA Comments/Feedback
- Produce Final Handbook and Report – end of August

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

Slide 25



Questions and Answers

Prepared for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

6/7/2001

Slide 26